(21) Application No 9311048.4

(22) Date of filing 28.05.1993

(30) Priority data
(31) 9211648   (32) 02.06.1992   (33) GB

(71) Applicant
Racal-Datacom Limited

(Incorporated in the United Kingdom)

Western Road, Bracknell, Berkshire, RG12 1RG,
United Kingdom

(72) Inventor
Simon Anthony Blair Avarne

(74) Agent and/or Address for Service
R W Obee
Racal Group Services Limited,
Group Patents Department, Richmond Court,
309 Fleet Road, Fleet, Hampshire, GU13 8BU,
United Kingdom

(51) INT CL⁵
H04L 9/32

(52) UK CL (Edition L)
H4P PDCSA
G4A AAP

(56) Documents cited
US 5153919 A   US 4393269 A

(58) Field of search
UK CL (Edition L) H4P PDCSA PDCSX
INT CL⁵ H04L
Online databases: WPI, INSPEC, CLAIMS, JAPIO.

(54) **Data communication system**

(57) In a data communication system a plurality of users are equipped with respective devices for computation and authentication of message authenticators. Each device stores a common cryptographic function; a common secret key and a respective non-secret offset for the key. They are programmed to perform the functions of: (i) computing and outputting an authenticator for an entered message using the cryptographic function and key combined with the respective offset; and (ii) computing an authenticator for an entered message using the cryptographic function and key combined with any entered offset, comparing that authenticator with one received with the message and displaying a "pass" or "fail" decision. The devices are incapable of displaying or otherwise outputting any authenticator computed using any offset other than its respective stored offset, however. In this way it can be ensured that a transmitted authenticator can act as a verifiable "signature" to a message uniquely identifying the sender.
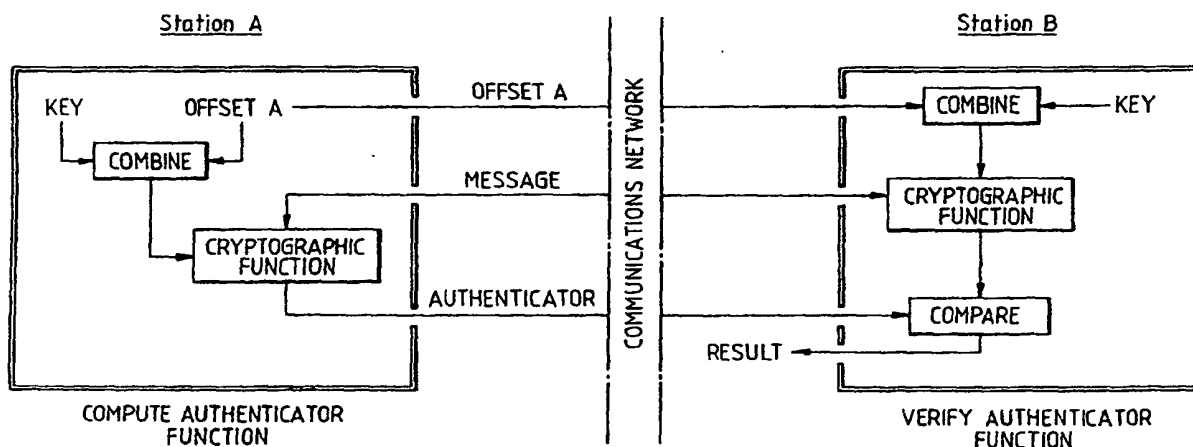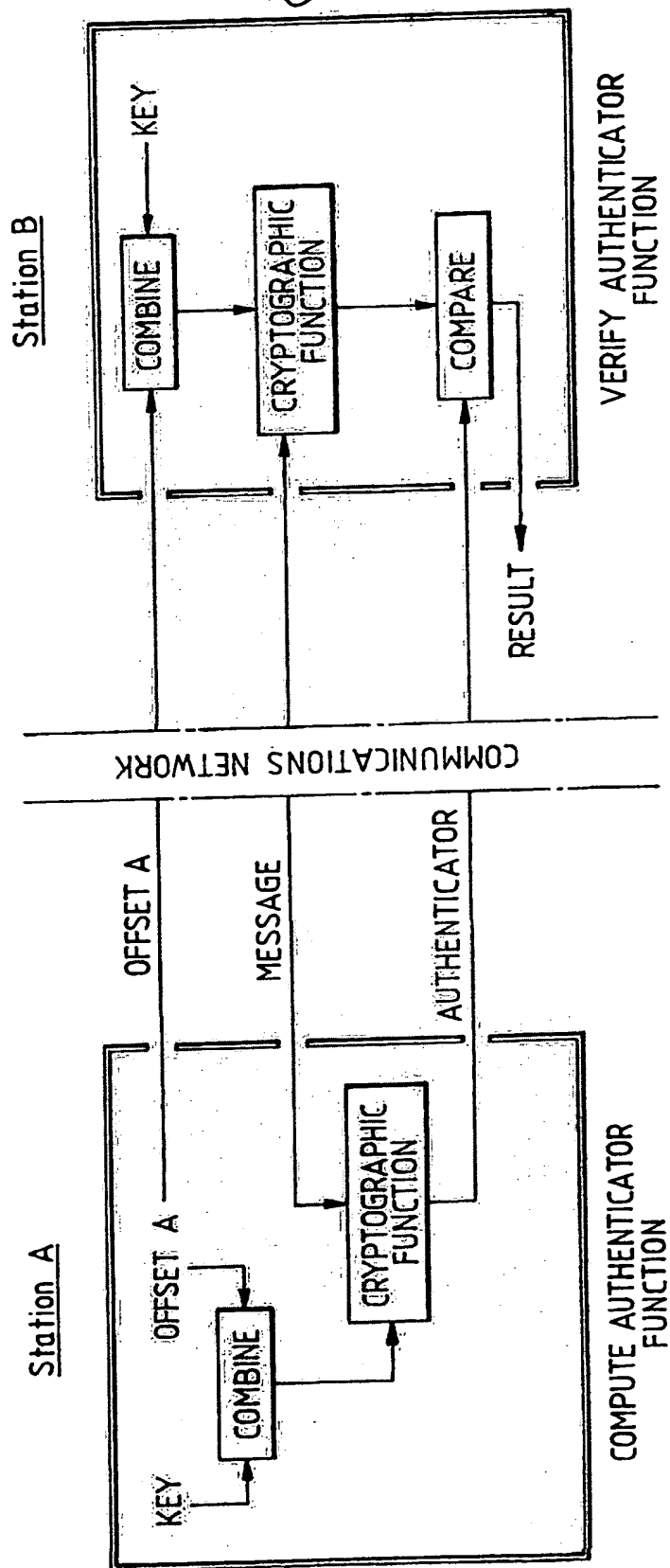
Fig.1.

Station A

Station B

COMPUTE AUTHENTICATOR
FUNCTION

VERIFY AUTHENTICATOR
FUNCTION

At least one drawing originally filed was informal and the print reproduced here is tak n from a later filed formal copy.

Fig.1.

1/3

Station B

KEY

COMBINE

CRYPTOGRAPHIC FUNCTION

COMPARE

RESULT

VERIFY AUTHENTICATOR FUNCTION

COMMUNICATIONS NETWORK

OFFSET A

MESSAGE

AUTHENTICATOR

Station A

KEY

OFFSET A

COMBINE

CRYPTOGRAPHIC FUNCTION

COMPUTE AUTHENTICATOR FUNCTION

Fig.2.

2/3

Station B

VERIFY RESPONSE FUNCTION

Station A

COMPUTE RESPONSE FUNCTION

COMMUNICATIONS NETWORK

KEY

COMBINE

CRYPTOGRAPHIC FUNCTION

COMPARE

RESULT

CHALLENGE

OFFSET A
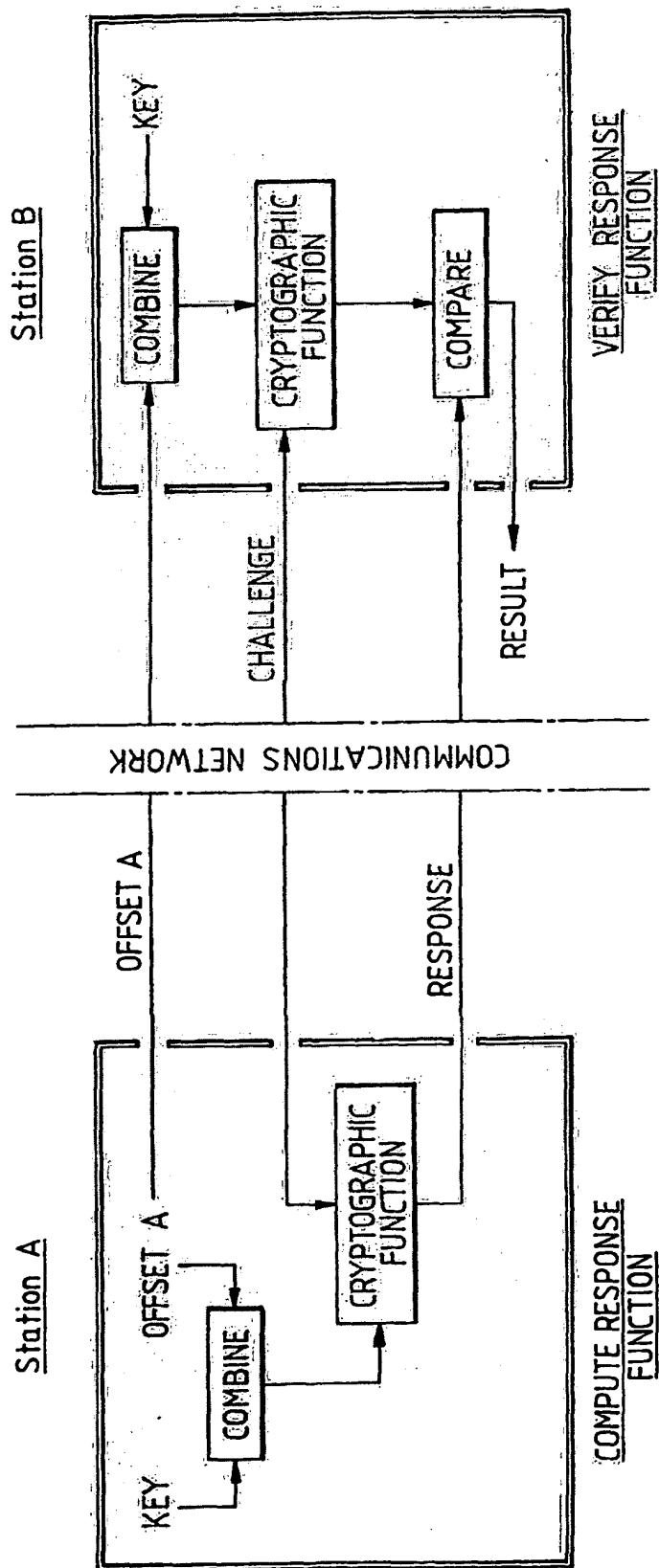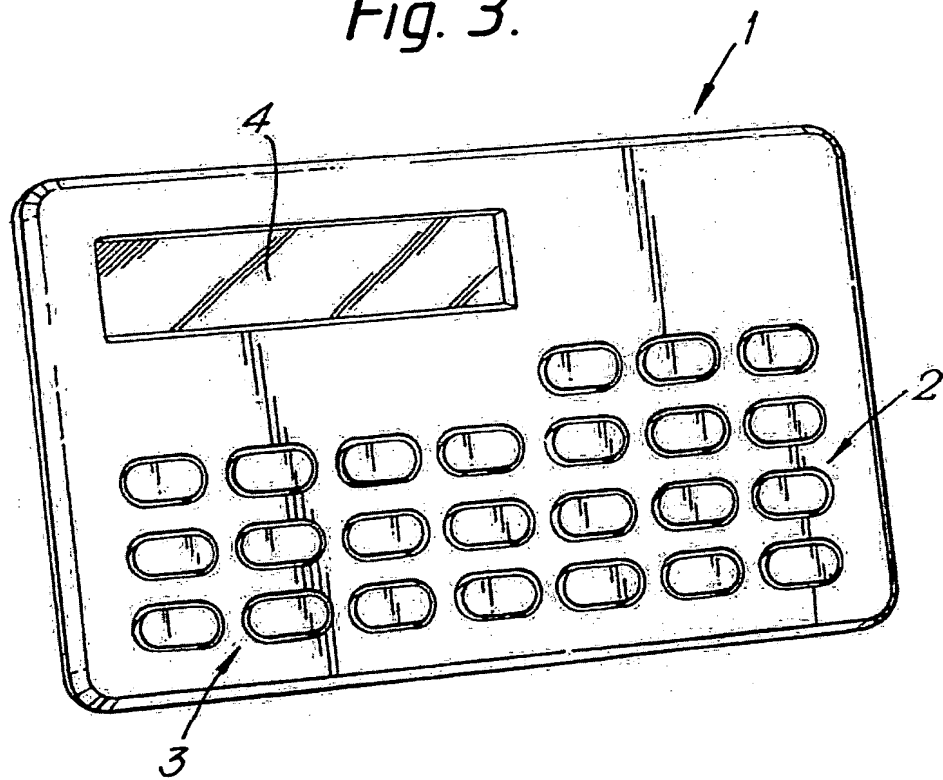
RESPONSE

KEY

OFFSET A

COMBINE

CRYPTOGRAPHIC FUNCTION

Fig. 3.

5

Data Communication System

10

The present invention relates to data communications and more particularly is concerned with techniques for the authentication both of messages flowing across a communications network and of their senders - factors of

15 great importance e.g. in the field of electronic funds-transfer and for other systems carrying financial or other commercially-sensitive information.

In such systems it is clearly important to be able to

20 detect at the receiving end any active attack upon, or other corruption of, a message which might have taken place in the course of its transmission across the network.   An active attack might take the form of an interceptor adding, removing or altering information in

25 the message with criminal or vexatious intent.   While it may be almost impossible to prevent an active attack there are various mechanisms which aim to ensure that such an attack will be detected and hence can be rendered nugatory.   The most common depends upon the generation,

30 prior to transmission, of a cryptographic check-sum or message authentication code - termed herein an "authenticator" - from the information contained in the message, which is then appended to the message for transmission.   The theory underlying this approach is

35 that if the recipient himself computes the expected authenticator from the message as received using the same cryptographic transformation, and finds it to disagree with the authenticator actually received with the message, then he will know that the message has been

altered in some way.   If on the other hand the expected
and received authenticators match then he knows with a
high degree of probability that the message has not been
altered, that probability increasing with the length of
5   the authenticator.   An example of this in common usage
is the system described in American National Standards
Institute (ANSI) standards X9.9 and X9.19.   Within these
standards the cryptographic algorithm is the Data
Encryption Algorithm as described in ANSI X3.92, the
10   cryptographic key is a 56-bit DEA key and the
authenticator is a 32-bit value appended to the message.

The success of such a system of message authentication of
course depends on maintaining the secrecy of the
15   cryptographic key from would-be interceptors.   In any
such system the same key must, however, be known to, or
at least available for the computation of authenticators
by, both the sender and recipient.   In known systems
this raises the possibility that one user might
20   impersonate another and, since the foregoing possibility
exists, that a user might attempt to repudiate a genuine
transaction.   That is to say, while a recipient may be
certain from the contents of a received authenticator
that any given message was received in the form in which
25   it was originally sent, the authenticator itself cannot
guarantee that the sender was the person whom the message
purports it to be because the same authenticator
generating key is available to all users.

30   The present invention seeks to address this problem and
accordingly in one aspect resides in a data communication
system in which a plurality of users are equipped with
respective devices each for the computation and for the
verification of message authenticators;   each such device
35   storing a common cryptographic function, a common secret
cryptographic key and a respective non-secret offset for
said key;   and each such device being programmed to
perform selectably the functions of: (i) computing and
outputting an authenticator for a message inputted to the

device, using said cryptographic function and said key combined with the respective stored offset; and (ii) computing an authenticator for a message inputted to the device, using said cryptographic function and said key

5   combined with an inputted offset, comparing that authenticator with an authenticator inputted to the device and outputting an indication of verification or non-verification based on said comparison; but each said device being incapable of outputting an authenticator

10   computed using said cryprographic function and said key combined with any offset other than its respective said stored offset. An "offset" in this invention is a value which effectively modifies the common cryptographic key in a respective manner.

15

In the operation of this system for message authentication a received authenticator will only be verified by a recipient if he has performed the aforesaid function (ii) using the key offset which corresponds to

20   the device of the sender of the message. An essential feature of the system, however, is that the only user who can output (and thus transmit) an authenticator using the offset which corresponds to his own device is that user himself. The authenticator can therefore act as a

25   verifiable "digital signature" identifying the sender of a message, the value of this offset effectively being the sender's ID within the system.

It is important that the (unmodified) common key stored

30   in the devices of this system remains secret, but the offsets corresponding to respective users need not. Indeed the sender's respective offset must be made known to the recipient in order for him to perform the authenticator verification function. If a user should

35   send a message with an authenticator computed with his own device and respective offset but purports to be some other user, however, th receiv d authenticator will not match the authenticator computed by the recipient using the purported user's offset and he will therefore know

that the message is not genuine. Furthermore, the
knowledge of users' offsets by an unauthorised person
does not provide any means for subverting the system
without knowledge also of the common key.

5

The invention also resides per se in an aforesaid device
for use in the above-defined system. In a preferred
embodiment each such device is in the form of a portable
token akin to a hand-held calculator, having a key pad
10 for the entry of message data, authenticators to be
verified and corresponding offset values, and for
entering the commands to perform the aforesaid functions
(i) and (ii), and a display for indicating computed
authenticators and verification or non-verification
15 decisions. Additionally or alternatively an electrical
interface may be provided for the direct input and output
of messages and authenticators from/to an associated
terminal apparatus. The physical and electrical
construction of the token should be such as to prevent
20 anyone from reading the secret common key, changing the
stored offset value or changing the functionality of the
token - and in particular from deriving an output of any
authenticator computed during the first phase of the
above-defined verification function (ii). In practice
25 this can readily be achieved by implementing all of the
token's functions in a single microprocessor chip.

In another aspect of the invention, since any message
with its corresponding authenticator will serve to verify
30 its sender the same equipment as provided in the above-
defined system can be used primarily for the purpose of
verifying members of a group using a communications
network, in circumstances which do not require the
authentication of messages as such, but where possession
35 of an authorised device is a prerequisite to membership
of the group. For example there can be considered a
distributed database system to which a large number of
different users may wish to obtain access. Each
database operator might not need to know the individual

identities of all of the users who may request access at any time but does need to know that any person to whom access is to be given has been authorised by the allocation of a said device.   In this aspect the user

5   who wishes to verify the authenticity of another user generates a random number which is issued as a "challenge" to that user.   This number is then processed by that user in accordance with function (i) of his device, where the "challenge" number constitutes the

10   inputted message in the invention as defined above, and outputs a "response" number (which constitutes the authenticator computed for that message).   This "response" number, together with that user's offset, is then transmitted to the first user who uses his own

15   device (or equivalent) to perform the verification function (ii) of the invention where the "challenge" number constitutes the inputted message and the "response" number constitutes the inputted authenticator.

20   The invention will now be more particularly exemplified with reference to the accompanying drawings in which:-

Figure 1 is a diagram illustrating the functions performed in computing and verifying an authenticator in

25   connection with the transmission of a message in a system according to the invention;

Figure 2 is a diagram illustrating the functions performed in computing and verifying a response to an

30   identification challenge in a system according to the invention;   and

Figure 3 is a perspective view of an individual token for use in a system according to the invention.

35

Referring to Figure 1, this illustrates two user stations A and B within an overall data communication system comprising many such stations between which messages are sent, e.g. payment instructions within a banking network.

At each station the user is equipped with a respective
electronic token for use in computing authenticators to
be appended to messages sent by that user and for
verifying authenticators received with messages from
5   other users.   Each such token has been initialised with
a common cryptographic function (e.g. the Data Encryption
Algorithm of ANSI X3.92), a common secret cryptographic
key and an individual offset value for that key.   Each
token has also been programmed to perform two distinct
10   functions, namely: (i) to compute and display an
authenticator from an inputted message using the common
cryptographic function and the common key as modified by
that token's own stored offset;   and (ii) to compute an
authenticator from an inputted message using the common
15   cryptographic function and the common key as modified by
an inputted offset, compare it with an inputted
authenticator and display the result of that comparison
as a pass or fail;   but it cannot perform any other
function using the secret key.   In particular, the token
20   cannot display or otherwise output any authenticator
computed in the course of its verification function (ii),
but can only compare it as aforesaid and display the
result.

25   An individual token for use in this system may take the
form indicated in Figure 3, namely a hand-held device 1
similar in appearance to a conventional personal
calculator (the usual functions of which it may also
perform).   A keypad 2 is provided for the entry of data
30   and a series of function keys 3 for entry of the commands
appropriate to its operation.   A liquid crystal display
4 is provided for checking the entered data, issuing
prompts and displaying authenticators and pass/fail
decisions.   Preferably operation of the token itself
35   requires entry of a user-defined PIN, to minimise the
risk of its misuse if lost or stolen.

Returning to Figure 1 it is assumed that the us r at
station A has a message to send to station B.   He enters

the message into his token and enters the command for the
token to perform its computation function (i). The
message is therefore encrypted under the common key as
modified by that token's stored offset (offset A) to
5 produce and display a corresponding authenticator. The
message, together with this authenticator and the value
of the offset A is then transmitted over the
communications network to station B. The user at
station B wants to verify that the message has been
10 received without alteration and also to verify that the
sender of the message is who it is purported to be,
namely user A. He therefore enters the message, the
received authenticator and the received offset A into his
own token and enters the command for the token to perform
15 its verification function (ii). The message is
therefore encrypted under the same key as modified by the
same offset as in the user A's token to produce (but not
display) an authenticator which is then compared with the
received authenticator, and if it matches the token
20 displays a "pass" result. By this means user B can be
confident that the message has been received without
alteration. Since he also knows that the sender of the
message must have had the authenticator displayed to him
in order to transmit it and that the only token which can
25 display that authenticator in response to that message is
the one which has been initialised with offset A then he
can also be confident that it was actually sent by user
A.

30 These same tokens can be used in any other communication
system where users wish to be able to verify the identity
of other users but without necessarily involving message
authentication as such. An example of this is shown in
Figure 2. In this case the user at station B wishes to
35 verify that the user at station A is an authorised user
of the network. He accordingly uses an additional
function of his token to generate and display a random
number, which is transmitted to user A as a "challenge".
User A then uses his token to encrypt that number under

the common key as modified by his offset A to produce and
display a "response" number. He transmits this number
together with the value of his offset A to user B who
enters them into his token and performs the same
5 verification function as if the original "challenge"
number was a received message and the "response" number
was the corresponding authenticator. If a "pass" result
is displayed, he similarly knows that user A is genuine
because only that user could have had knowledge of the
10 given "response" from the "challenge" using offset A in
the encryption.

CLAIMS

1. A data communication system in which a plurality of
users are equipped with respective devices each for the
5   computation and for the verification of message
authenticators; each such device storing a common
cryptographic function, a common secret cryptographic key
and a respective non-secret offset for said key; and
each such device being programmed to perform selectably
10 the functions of: (i) computing and outputting an
authenticator for a message inputted to the device, using
said cryptographic function and said key combined with
the respective stored offset; and (ii) computing an
authenticator for a message inputted to the device, using
15 said cryptographic function and said key combined with
any inputted offset, comparing that authenticator with an
authenticator inputted to the device and outputting an
indication of verification or non-verification based on
said comparison; but each said device being incapable of
20 outputting any authenticator computed using said
cryptographic function and said key combined with any
offset other than its respective said stored offset.

2. A method of transmitting and verifying a message
25 from a first user to a second user in a data
communication system according to claim 1, which
comprises the steps of: the first user operating a first
said device to compute and output an authenticator for
the message to be transmitted, by performing the said
30 function (i); transmitting to the second user the
message, the authenticator computed therefor and the
identity of the respective offset stored in the first
said device; and the second user operating a second said
device to verify the authenticator received from the
35 first user, by performing the said function (ii) with
said key combined with the offset identified with the
first said device.

3.   A method of verifying a first user to a second user
in a data communication system according to claim 1,
which comprises the steps of: the second user generating
a random message and transmitting the same to the first
5   user;   the first user operating a first said device to
compute and output an authenticator for said random
message, by performing the said function (i);
transmitting to the second user the authenticator
computed for said random message and the identity of the
10   respective offset stored in the first said device;   and
the second user operating a second said device to verify
the authenticator received from the first user, by
performing the said function (ii) with said key combined
with the offset identified with the first said device.
15

4.   A device for a user of a data communication system
to compute and verify message authenticators, the device
comprising: means storing a cryptographic function
common to the users of the system, a secret cryptographic
20   key common to the users of the system and a respective
non-secret offset for said key;   input means for messages
to be sent by the user or received from other users and
for offsets and authenticators received from other users;
output means for authenticators to be transmitted by the
25   user and for indicating verification or non-verification
of authenticators received from other users;   and
processing means adapted to perform at the selection of
the user the functions of: (i) computing and outputting
an authenticator for a message inputted to the device,
30   using said cryptographic function and said key combined
with the respective stored offset;   and (ii) computing an
authenticator for a message inputted to the device, using
said cryptographic function and said key combined with
any inputted offset, comparing that authenticator with an
35   authenticator inputted to the device and outputting an
indication of verification or non-verification based on
said comparison;   but said device being incapable of
outputting any authenticator computed using said

cryptographic function and said key combined with any offset other than its respective said stored offset.

5. A data communication system substantially as hereinbefore described with reference to the accompanying drawings.

Pat nts Act 1977 Examin r's r port to the Comptroller under Section 17 (The Search Report)	Application number GB 9311048.4

Relevant Technical fields	Search Examiner
(i) UK Cl (Edition L) H4P(PDCSA,PDLSX) (ii) Int Cl (Edition 5) HD4L	DR E PLUMMER

Databases (see over) (i) UK Patent Office (ii) ONLINE DATABASES: WPI, INSPCE, CLAIMS, JAP1D	Date of Search 17 AUGUST 1993

Documents considered relevant following a search in respect of claims   ALL

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
A	US 5153919 AT & T	
A	US 4393269 IBM	

Category	Identity of document and relevant passages	Relevant to claim(s)

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).